Midyear in Review:

2013 January-June Threat Landscape Report

The first half of 2013 has been a busy one at FortiGuard Labs. We've seen old threats continue to be exploited, new threats emerge, and mobile malware explode in growth. We're excited to share with you a recap of some of our findings and research so far in 2013. At the end of this report, you'll also find a special technical report on the two massive cyber attacks impacting South Korea this year.

2013 Threat Predictions: Midyear in Review

FortiGuard Labs issues an annual set of threat predictions, based on trends the team is actively monitoring globally. This year's predictions, first published in December 2012, are below and include how they've played out at the midyear mark.

Prediction 1: APTs Target Individuals through Mobile Platforms

APTs, also known as Advanced Persistent Threats, are defined by their ability to use sophisticated technology and multiple methods and vectors to reach specific targets to obtain sensitive or classified information. The most recent examples include Stuxnet, Flame and Gauss. In 2013 we predict we'll see APTs targeted at the civilian population, which includes CEOs, celebrities and political figures. Verifying this prediction will be difficult, however, because after attackers get the information they're looking for, they can quietly remove the malware from a target device before the victim realizes that an attack has even occurred. What's more, individuals who do discover they have been victims of an APT will likely not report the attack

The first half of 2013 has seen a number of old vulnerabilities still being exploited on unpatched systems, the emergence of a new threats and a marked increase in the amount mobile malware coming into the labs daily.

In the following whitepaper, we're going to examine:

* The threat predictions FortiGuard Labs made at the end of 2012 and how accurate they were (or weren't) at the midyear mark.
* The increase of mobile malware on Android devices including new mobile ransomware
* The continued proliferation of the ZeroAccess botnet and which countries are seeing the biggest infection rates
* The Citadel botnet takedown
* Patched vulnerabilities in Ruby on Rails, Java, Adobe Acrobat and Apache that are still being exploited on unpatched systems
* The lowdown on April's Spamhouse DDoS attack
* And a special, in-depth look at the latest South Korean cyber attacks

to the media. Because these attacks will first affect individuals and not directly critical infrastructure, governments or public companies, some types of information being targeted will be different. Attackers will look for information they can leverage for criminal activities such as blackmail; threatening to leak information unless payment is received.

Result So Far: There has not been an incident so far this year that can confirm this prediction.

Prediction 2: Two Factor Authentication Replaces Single Password Sign on Security Model

The password-only security model is dead. Easily downloadable tools today can crack a simple four or five character password in only a few minutes. Using new cloud-based password cracking tools, attackers can attempt 300 million different passwords in only 20 minutes at a cost of less than $20 USD. Criminals can now easily compromise even a strong alphanumeric password with special characters during a typical lunch hour. Stored credentials encrypted in databases (often breached through Web portals and SQL injection), along with wireless security (WPA2) will be popular cracking targets using such cloud services. We predict next year we'll see an increase in businesses implementing some form of two-factor authentication for their employees and customers. This will consist of a Web-based login that will require a user password along with a secondary password that will either arrive through a user's mobile device or a standalone security token. While it's true that we've seen the botnet Zitmo recently crack two-factor authentication on Android devices and RSA's SecurID security token (hacked in 2011), this type of one-two punch is still the most effective method for securing online activities.

Result So Far: So far in 2013, the push toward two-factor authentication has been substantial, as has the amount of coverage in the press introducing regular Internet users to the technology. Some big Internet properties such as Twitter, Microsoft's Outlook.com, Dropbox, Evernote and Facebook have all introduced some type of multi-factor authentication to their products.

Prediction 3: Exploits to Target Machine-to-Machine (M2M) Communications

Machine-to-machine (M2M) communication refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. It could be a refrigerator that communicates with a home server to notify a resident that it's time to buy milk and eggs, it could be an airport camera that takes a photo of a person's face and cross references the image with a database of known terrorists, or it could be a medical device that regulates oxygen to an accident victim and then alerts hospital staff when that person's heart rate drops below a certain threshold. While the practical technological possibilities of M2M are inspiring as it has the potential to remove human error from so many situations, there are still too many questions surrounding how to best secure it. We predict next year we will see the first instance of M2M hacking that has not been exploited historically, most likely in a platform related to national security such as a weapons development facility. This will likely happen by poisoning information streams that transverse the M2M channel -- making one machine mishandle the poisoned information, creating a vulnerability and thus allowing an attacker access at this vulnerable point.

Result So Far: In June, both the FDA and ICS-CERT issued advisories about potential issues with many types of medical devices such as pacemakers, insulin pumps and implanted defibrillators. While there are no known incidents of these devices being exploited in the wild, many researchers have discovered numerous flaws in devices and have demonstrated proofs of concept of malicious attacks on these devices.

Prediction 4: Exploits Circumvent the Sandbox

Sandboxing is a practice often employed by security technology to separate running programs and applications so that malicious code cannot transfer from one process (i.e. a document reader) to another (i.e. the operating system). Several vendors including Adobe and Apple have taken this approach and more are likely to follow. As this technology gets put in place, attackers are naturally going to try to circumvent it. FortiGuard Labs has already seen a few exploits that can break out of virtual machine (VM) and sandboxed environments, such as the Adobe Reader X vulnerability. The most recent sandboxing exploits have either remained in stealth mode (suggesting that the malware code is still currently under development and test) or have actively attempted to circumvent both technologies. Next year we expect to see innovative exploit code that is designed to circumvent sandbox environments specifically used by security appliances and mobile devices.

Result So Far: in April, the Polish group Security Explorations demonstrated exploits in Java that allowed complete sandbox circumvention. Adobe also patched exploits in Acrobat Reader that allowed a sandbox to be circumvented,. As of this writing,the Group-IB reports there is another exploit in Adobe Reader that has not been patched. Group-IB has not provided proof of concept to Adobe.

Prediction 5: Cross Platform Botnets

In 2012, FortiGuard Labs analyzed mobile botnets such as Zitmo and found they have many of the same features and functionality of traditional PC botnets. In 2013, the team predicts that thanks to this feature parity between platforms, we'll begin to see new forms of Direct Denial of Service (DDoS) attacks that will leverage both PC and mobile devices simultaneously. For example, an infected mobile device and PC will share the same command and control (C&C) server and attack protocol, and act on command at the same time, thus enhancing a botnet empire. What would once be two separate botnets running on the PC and a mobile operating system such as Android will now become one monolithic botnet operating over multiple types of endpoints.

Result So Far: While we haven't see a bona fide cross platform botnet, we have seen a piece of Android malware that attempts to infect a Windows PC if it is connected and has autorun enabled. It is likely the author(s) of this malware will attempt to make this more robust in the future or attempt other methods to infect a PC through an infected Android device.

Prediction 6: Mobile Malware Growth Closes in on Laptop and Desktop PCs

Malware is being written today for both mobile devices and notebook/laptop PCs. Historically, however, the majority of development efforts have been directed at PCs simply for the fact that there are so many of them in circulation, and PCs have been around a much longer time. For perspective, FortiGuard Labs researchers currently monitor approximately 50,000 mobile malware samples, as opposed to the millions they are monitoring for the PC. The researchers have already observed a significant increase in mobile malware volume and believe that this skewing is about to change even more dramatically starting next year. This is due to the fact that there are currently more mobile phones on the market than laptop or desktop PCs, and users are abandoning these traditional platforms in favor of newer, smaller tablet devices. While FortiGuard Labs researchers believe it will still take several more years before the number of malware samples equals what they see on PCs, the team believes we are going to see accelerated malware growth on mobile devices because malware creators know that securing mobile devices today is currently more complicated than securing traditional PCs.

Result So Far: While mobile malware continues to

explode in growth, PC-based malware continues to rule the roost in the world of malware. We expect to see mobile-based attacks continue their acceleration in the second half of 2013.

2012 Flashback: Ransomware Moves to the Mobile World

In December 2011, FortiGuard predicted ransomware would migrate over to mobile devices to take them hostage in 2012 Over the past few years, FortiGuard Labs has witnessed the evolution and success of "ransomware" (an infection that holds a device "hostage" until a "ransom" payment is delivered) on the PC. Mobile malware that utilize exploits have also been observed, along with social engineering tricks that lead to root access on the infected device. With root access comes more control and elevated privileges, suitable for the likes of ransomware.

Result So Far: While we didn't see any mobile ransomware in 2012, the first half of 2013 has shown that our predictions were spot-on. The FakeDefender malware has started to target Android devices; its operation and intent are virtually identical to ransomware that is common to the desktop PC.

Mobile Malware

Until recently, Bring Your Own Device (BYOD) wasn't an initiative that companies were considering. Employees used an assigned laptop, and if there was a need for an employee to have email on-the-go, they were either given a cellular modem for their laptop or a locked-down smartphone, often a Blackberry device.

Today, BYOD has been embraced by many companies. Employees, especially younger workers new to the workforce, have demanded the option to use technology that they feel most comfortable with. Efficiency and productivity gains are commonplace in organizations that have adopted a BYOD strategy.

But with this strategy comes risk. Companies are fearful of sensitive corporate information leaking from their networks through employees' personal devices, and rightly so.

One of the largest risks in the world of BYOD is that of mobile malware. As recently as a few years ago, mobile malware wasn't much of a concern; most malware targeting smart phones were nothing more than annoyware or scam software that could commit SMS fraud or the like.

The overwhelming success and adoption of smartphones in the marketplace has led to a complete change of reality in the world of mobile security: quite simply, mobile malware has exploded and shows no signs of abating anytime soon.

In 2009, the majority of mobile malware in existence targeted Symbian – which made perfect sense then: iOS and Android were still relatively new in the marketplace compared to their competition, and a large number of the malware was coded by programmers in Eastern Europe and China, places where Symbian commanded a large share of the installed user base.

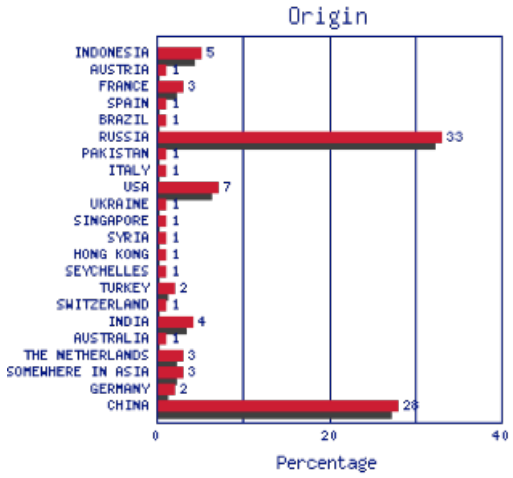


Figure: Origin of Mobile Malware, 2009

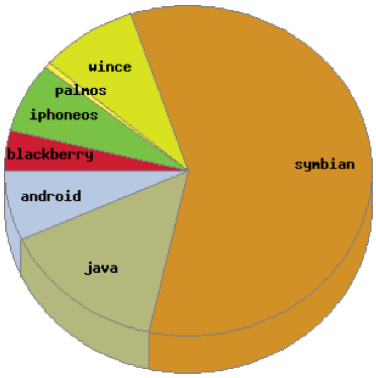


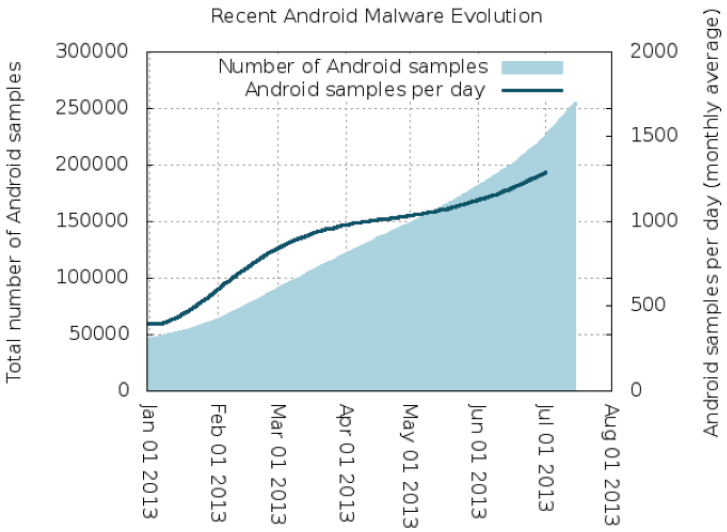
Figure: Distribution of Mobile Malware, 2009

In 2013, though, the environment has changed dramatically. Wide scale manufacturer adoption of Google's Android OS globally has led to an explosion of smartphones in the marketplace. Android devices are available in every market, at price levels from the incredibly inexpensive to feature-rich, bleeding-edge computing monsters.

Coupled with the explosion of available applications to extend device functionality, cybercriminals and other nefarious types have used this platform as a new business opportunity.

FortiGuard is currently tracking over 300 unique families of Android mobile malware, and over 250,000 unique malicious Android samples.

The acceleration of malware development is also increasing. At the beginning of 2013, FortiGuard was processing just under 1,000 new samples every day. By the start of Q2 2013, we crossed the 1,000 per day barrier. At the end of Q2, we reached a staggering 1,300 new samples per day. That's a 30% increase in just six months.



We expect this accelerated growth to continue into the second half of 2013.

The Birth of Mobile Ransomware

FakeDefender brings ransomware to Android

In June we saw a new piece of Android malware, one that pretends to provide malware and virus protection to the victim's phone. Much like fake antivirus applications on the PC, FakeDefender is actually malware and will attempt to trick its victim into purchasing a fake antivirus solution in order to clean up false infections reported by the malware.

About six hours after FakeDefender is installed, it will lock the victim's phone with an image of pornography and a link to purchase software that will clean up the phone. It also searches for key files on the phone and erases them, in the hopes of preventing restoration of the phone from a backup file.

Much like its PC-based cousins, FakeDefender victims without a backup of their phone are left with two options: pay the ransom, or wipe the phone and lose all the contents of the phone.

We expect to see more variants and new families of ransomware to target Android devices in the second half of the year.

Botnet Update

ZeroAccess Keeps Marching

In April's Threat Landscape Report, we shared that the cybercriminals behind the ZeroAccess botnet were making great strides (and spending a significant amount of money) maintaining the size of their botnet. We reported a staggering 100,000 new infections on average per week.

Our observations and surveillance of ZeroAccess shows that this pace has not slowed in the last three months: ZeroAccess's owners continue to pay their infection affiliates a significant amount of money to keep the 100,000 new infections per week going.

As older infected computers get disinfected, new ones are made available to continue in their illicit cash generation.

We have determined that there are four main ZeroAccess bots in operation:

- A 32-bit version, which is used to commit click fraud
- A 32-bit version, used to mine Bitcoin
- A 64-bit version, used for click fraud
- A 64-bit version, used to mine Bitcoin

It's clear the people behind this botnet are trying to capture as many infections as they can in order to continue generating income.

The United States continues have the highest number of infections, but make no mistake, ZeroAccess is a true global botnet: databases reveal significant infections in Japan, India, Romania, Brazil, Italy, Taiwan, Canada, Russia, Germany, Venezuela and Argentina.

Comparing infections in January and June of this year, it's clear that ZeroAccess recruits affiliates from around the globe in order to diversify how and where it makes money.

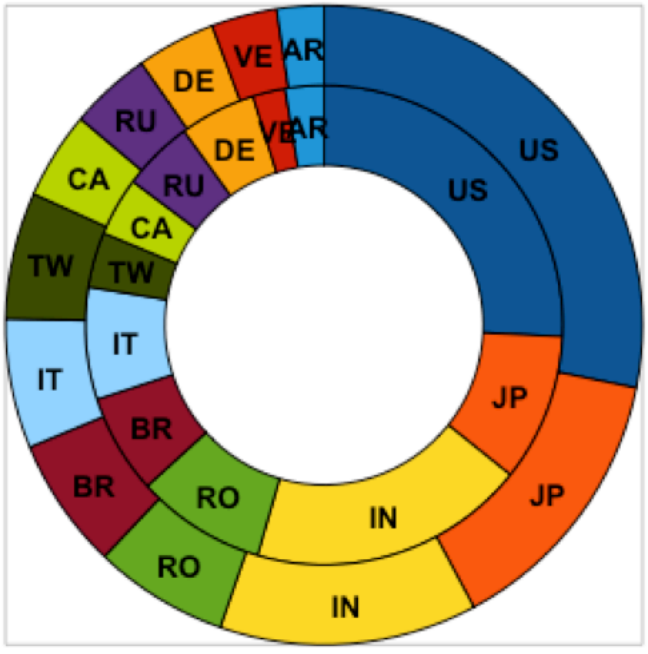


Figure: ZeroAccess Infections by Geographic Location, January (inner ring) vs. June

Citadel Takedown

In June, Microsoft's Digital Crimes Unit, working with the FBI and the U.S. courts, took a huge chunk out of the capabilities of the Citadel botnet.

Citadel is a ZeuS variant that is responsible for infecting what is believed to be millions of computers around the world in the hopes of stealing financial information through key logging and form grabbing and using that information to steal money from the bank accounts of infected victims.

This latest takedown, known as Operation b54, disrupted the operation of over 1,400 different Citadel botnets almost simultaneously. While that indeed is a staggering number, it most certainly doesn't spell the end of Citadel or the theft of money from infected computers. The very nature of crimeware kits and how incredibly easy it is for cybercriminals to set up new versions of Citadel means that others will undoubtedly take the place of these.

An interesting side story to Operation b54 is that there are some reports this takedown may have had some collateral damage. A number of security researchers have reported that a number of the domains seized by Microsoft (a procedure known as sinkholing) were already sinkholed and being used to research Citadel.

Sadly, as with many other botnets that are taken down – such as Mariposa, Citadel will likely rise again.

Other Incidents of Note

Ruby on Rails Remote Code Execution

In January, it was announced that a critical vulnerability in the Ruby on Rails Framework that could give a remote attacker the ability to execute code on the underlying Web server.

Ruby on Rails (RoR) is a Web application framework for the Ruby programming language. Put simply, it allows for rapid, easy and elegant deployment of "Web 2.0" Websites. RoR is a popular framework: hundreds of thousands of Websites use RoR in

some fashion.

Further adding to the problem, a Metasploit module was made available to scan for the vulnerability, making the ability to find a Web server to exploit a trivial matter.

The exploit involved a flaw in the XML processor deserialization routine, which is used to create Ruby objects on the fly. RoR was patched to correct the flaw, but four months later it was discovered that an attacker or attackers was searching for, and exploiting, unpatched Web servers in order to infect them with software.

Java Remote Code Execution

In January, a zero-day exploit that was able to bypass Java's sandbox and run arbitrary Java code was discovered.

Java is a ubiquitous technology online – most computers have some form of Java installed and enabled. The vulnerability allowed a malicious applet to run any Java program, bypassing Java's sandbox and granting full access to the vulnerable computer.

Attacks were discovered in the wild and the exploit was quickly integrated into many popular crimeware attack kits, such asBlackHole, Redkit and Nuclear Pack, giving purchasers of these kits the ability to take advantage of the exploit and install malware on computers. A Metasploit module was also created for the vulnerability, making the ability to find victims a simple point and click affair.

The exploit involved a flaw in a JMX (Java Management Extensions) component that allowed the malicious applet to elevate its privileges and run any Java code it wished.

Oracle was quick to release a patch for the flaw – but similar to other exploits integrated into crimeware kits, many new victims were found – and continue to be found – running unpatched versions of Java, allowing malware to be installed.

Acrobat/Acrobat Reader Zero-Day in the Wild

In February, a PDF pretending to be a travel visa form from Turkey was detected circulating in the wild andtook advantage of a previously unseen vulnerability in Adobe's Reader software. The exploit worked with all recent versions of Adobe Reader (9.5.X, 10.1.X, and 11.0.X), and on most versions of Microsoft Windows, including 64-bit Windows 7 and most Mac OS X systems.

The exploit PDF was used by cybercriminals in order to install malware on their target's computers.

Adobe released a patch for the flaws in Reader on February 20th, but cybercriminals continue to use repackaged versions of the exploits online in spear-phishing attacks.

Massive DDoS Attack on Spamhaus

In April, botnet owners launched a massive DDoS attack on Internet spam fighter Spamhaus, content delivery provider CloudFlare and other Internet infrastructure providers.

The Spamhaus Project provides blacklisting services to many ISPs and email servers around the world with the intent of stopping the billions of spam emails sent daily. In February, Spamhaus added Dutch hosting provider CyberBunker to their blacklist for what Spamhaus said was for refusing to take action against spammers that Spamhaus believed were using CyberBunker to base their spamming operations. In retaliation for being added to Spamhaus' blacklist, groups launched a massive DDoS attack on Spamhaus and their infrastructure. It was believed that the attacks were launched at the behest of CyberBunker, but they were vehemently denied by CyberBunker. Other reports stated a loose alliance of hacktivists and cybercriminals collectively known as the STOPhaus Project were responsible.

The resources marshaled were staggering. The initial attack against Spamhaus peaked at an amazing 90 billion bits per second (Gbps). Spamhaus contacted content delivery and distributed DNS provider CloudFlare to assist in providing help in

keeping Spamhaus online.

CloudFlare was initially able to mitigate the attack, and Spamhaus was able to continue providing blacklist services to their subscribers. The attackers then stepped up their attacks again.

While multiple methods of DoS were used, the majority of the attack used what's known as a DNS amplification attack. Simply, bots send requests to an open DNS resolver asking for a copy of a larger DNS zone file. The attackers spoofed their IP addresses to appear to come from CloudFlare, which meant that the open DNS resolver sent the large file back to CloudFlare. Reports seem to show that a single bot sent a 36 byte request, which was replied to with a 3,000 byte reply - meaning the amplification was about 100 times the size of the request.

CloudFlare reported a staggering 150 Gbps of traffic at the attack's peak, and one Tier-1 provider reported peaks of twice that. The largest DDoS attacks on record previous to this attack had reached about 100 Gbps.

CDorked Attacks Apache

In late April, a new attack on the popular Apache Web server was discovered. Dubbed CDorked, it was able to compromise the Web server and redirect visitors of the compromised Web server to other servers that deliver malware using the BlackHole exploit kit. The attack may also have targeted the Lighttpd and Nginx Web server platforms.

CDorked shows many similarities to 2012's DarkLeech attack on Apache servers, but is significantly stealthier and smarter than DarkLeech was. Unlike DarkLeech, CDorked didn't load additional malicious modules on the infected server; instead it maliciously modified the existing httpd binary.

CDorked was interesting in that it did not write any information to the Web server's hard drive: everything was kept in memory and was accessed via obfuscated GET requests sent by the attackers to the compromised server. None of those GET requests were logged.

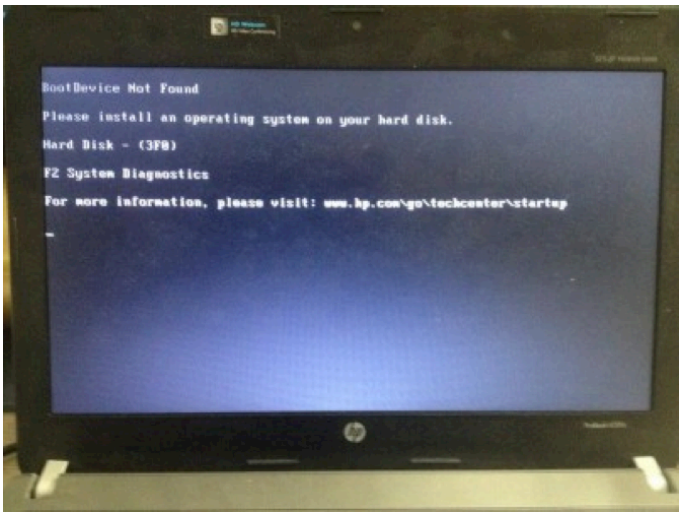
CDorked showed some intelligence in how it operated: it had a quota system built in. In other words, CDorked did not attempt to redirect each and every visitor to a BlackHole site. It also hid from users attempting to access administrative pages on the compromised Web server in an attempt to keep users who may have been more likely to notice a redirect to a crimeware delivery site from discovering the compromise.

Special Technical Report:

An In-Depth Analysis of the Attacks on South Korea

March 20 Wiper Attacks

On March 20th, 2013, at 2PM local time, several South Korean financial institutions and TV broadcast networks were hit with a particularly destructive piece of malware. The malware wiped hard drives on infected machines, preventing them from operating on reboot.



FortiGuard's AV analysis team provided substantial analysis of the malware and the attack. The attack made use of two different droppers. These droppers were used to place wipers on its infected system. Each dropper spawned two wipers (md5

sums below):

Dropper 1: `9263e40d9823aecf9388b64de34eae54`

Dropper 2: `b80153b66fdaafedfc0a65bcb940687d`

Wiper 1: `5fcd6e1dace6b0599429d913850f0364`

Wiper 2: `530c95eccdbd1416bf2655412e3dddbe`

Wiper 3: `db4bbdc36a78a8807ad9b15a562515c4`

Wiper 4: `0a8032cd6b4a710b1771a080fa09fb87`

Each wiper was designed to erase files, but would only trigger upon realization of a subset of the 3 following conditions, different for each wiper:

1. Absence of a specific File Mapping Object in memory

2. Absence of a specific temporary file

3. **Current Time > Present Time**.

Item 3 above is commonly known as a "time-bomb" malware.

Interestingly, the File Mapping Objects and temp files are apparently used by the wipers as simple mutexes, in order to not duplicate work in progress. They check for their existence, but do nothing with them. Another interesting note is that the File Mapping Objects didn't map an actual file: the mapped files have an invalid handle (-1)!

Once triggered, the wipers took the following actions:

1. Overwrote the Master Boot Record (MBR) of the infected host's hard drive with the string "HASTATI", "PRINCIPES" or "PR!NCPES". Hastati and Principes were classes of soldiers used in Roman times: Hastati was the first wave of soldiers in a battle and Principes were the second wave.

2. Depending on the Operating System version of the infected host, the wiper either wiped the entire hard drive with the same string or wiped each and every file on the host.

3. It also executed the following commands:

   a. `taskkill /F /IM pasvc.exe`

   b. `taskkill /F /IM clisvc.exe`

Both of these processes are popular Korean antivirus programs.

Wiper 1

Wiper 1 triggered on a File Mapping Object and a Time-Bomb:

File Mapping Object:

`JO840112-CRAS8468-11150923-PCI8273V`

Time-Bomb:

```
push    eax
call    dword ptr [esi+330h] ; GetLocalTime
mov     edi, 4DAD4678h  ; 2013-03-20 14:00:00
jmp     short loc_4011ED
-----------------------------------------------

                        ; CODE XREF: .text:004
push    0EA60h
call    dword ptr [esi+334h] ; sleep
lea     eax, [ebp-10h]
push    eax
call    dword ptr [esi+330h] ; GetLocalTime
```

If the infected computer doesn't have a File Mapping Object named as above and the local time of the computer is greater than 2013-03-20 14:00:00, it executed the following:

`taskkill /F /IM pasvc.exe`

`taskkill /F /IM clisvc.exe`

It then started a thread, which first overwrote the infected computer's MBR with the "HASTATI" string and then either overwrote the entire hard drive or each file on the computer with the same "HASTATI" string.

Finally, it executed the command `shutdown –r –t 0` in order to force a reboot of the infected computer, rendering it unusable.

Wiper 2

Wiper 2 triggered on a File Mapping Object, a Temp File and a Time-Bomb:

File Mapping Object:

`GOLD0112-CRAS8468-PAGE0923-PCI8273V`

Temp File: `windows\temp\kb01.tmp`

Time-Bomb:

```
add     esi, ecx
imul    esi, 64h
push    0EA60h          ; dwMilliseconds
add     esi, edx
call    edi ; Sleep
cmp     esi, 7D0Fh      ; 3-20 15:00:00
jb      short loc_10001070
```

If the compromised computer didn't have the File Mapping Object above, if the temp file above does not exist, and if its local time is greater than 03-20 15:00:00, it then started a thread that overwrote the entire HD with string "PR!NCPES." It then executed `shutdown -r -t 0` to force a reboot of the computer. There were no taskkill commands in this version. If the compromised computer didn't have the File Mapping Object but did have the temp file, it would sleep for a short time and then check for the file again.

Wiper 3

Wiper 3 triggered on a File Mapping Object and a Temp File:

File Mapping Object:

`JO840112-CRAS8468-11150923-PCI8273V`

Temp File: `windows\temp\~v3.log`

If the compromised computer didn't have the File Mapping Object above or the temp file, it executed the following commands:

```
taskkill /F /IM pasvc.exe
taskkill /F /IM clisvc.exe
```

It then started a thread that first overwrote the infected computer's MBR with the "PRINCIPES" string and then either overwrote the entire hard drive or each file on the computer with the same "PRINCIPES" string.

Finally, it executed the command `shutdown –r –t 0` in order to force a reboot of the infected computer, rendering it unusable.

Wiper 4

Triggered on File Mapping Object:

File Mapping Object name:

`JO840112-CRAS8468-11150923-PCI8273V`

If the compromised computer didn't have the File Mapping Object above, it executed the following commands:

```
taskkill /F /IM pasvc.exe
taskkill /F /IM clisvc.exe
```

It then started a thread that first overwrote the infected computer's MBR with the "PR!NCPES" string and then either overwrote the entire hard drive or each file on the computer with the same "PR!NCPES" string.

Finally, it executed the command `shutdown –r –t 0` in order to force a reboot of the infected computer, rendering it unusable.

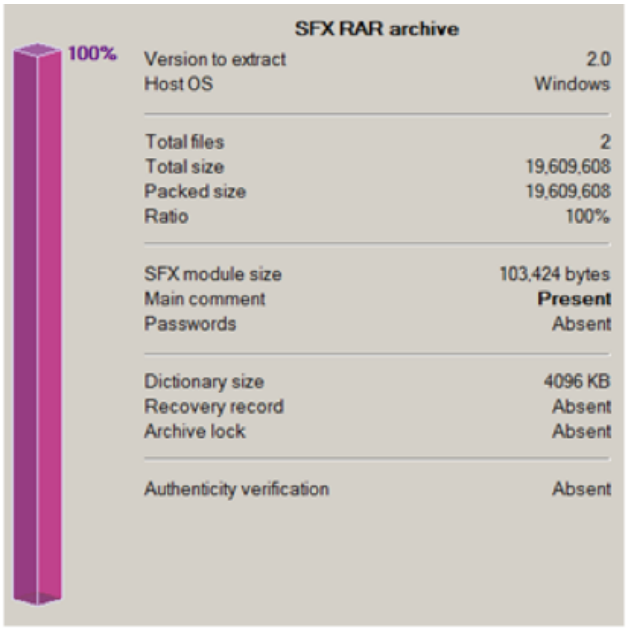
June 25 DNS DDoS Attacks

At or about 10:00am (local time) on June 25th, a large number of South Korean government Websites became inaccessible.

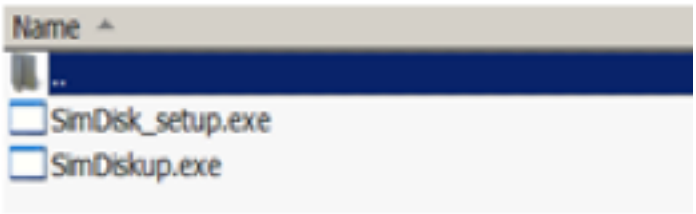
FortiGuard's AV analysis team determined the attacks were caused by specially crafted malware designed to perform DDoS attacks on two major South Korean DNS servers – ns.gcc.go.kr and ns2.gcc.go.kr.

During the team's investigation of the incident, they obtained a copy of the original attack sample that was served by a compromised Website (simdisk.co.kr).

The file, named `SimDisk_setup.exe`, turned out to be a self-extracting RAR file:



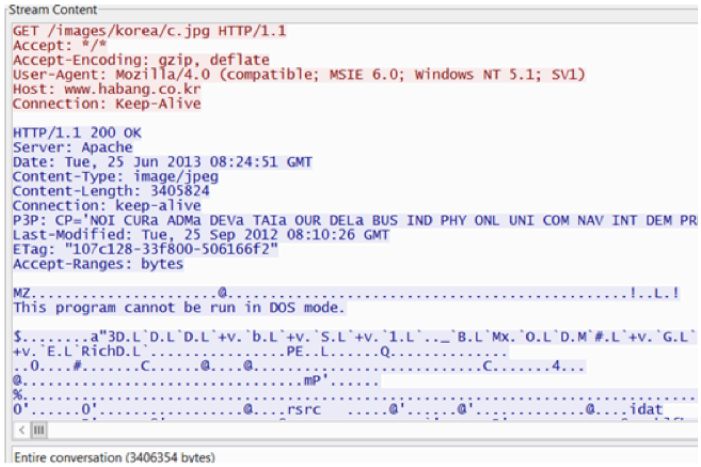
There were two files inside the self-extracting RAR file:



`SimDisk_setup.exe` is the actual installation file for SimDisk. `SimDiskup.exe`, created on June 24, is the malicious component.

```
B200 aSimdisk_exe_0  db '~simdisk.exe',0
B20D                 db    0
B20E                 db    0
B20F                 db    0
B210 aHttpWww_habang db 'http://www.habang.co.kr/images/korea/c.jpg'
```

`SimDiskup.exe` then attempted to download other malicious files from another Website. In this case, it downloaded `c.jpg`, which is actually an executable file. After it is downloaded, it is saved as `~simdisk.exe` and executed:



Once `~simdisk.exe`, formerly known as `c.jpg`, is executed, it drops 3 separate files:

Interestingly, `explorer.exe` and `config.ini` are actually the TOR system (version 0.2.3.25). The third file, `alg.exe`, is yet another downloader.

`Alg.exe` then used the TOR network to download another file, which is the final DDoS payload.

`Alg.exe` attempted to connect to the following TOR onions (an onion is a hidden, hard to trace Website that is accessible only via a TOR node):

`http://hfc4z2pxfdmsfczp.onion/etc/`

`http://n3fwfxcdjfv4zxpa.onion/etc/`

`http://p4dxzhnlukvh6p4a.onion/etc/`

`http://swe4ta6k64m7vguk.onion/etc/`

`http://7odyldjmpzjrhsye.onion/etc/`

`http://vtyee6ev7gki7qxf.onion/etc/`

`http://rns3d52wyctfktcb.onion/etc/`

`http://et53n5fxxmjukgki.onion/etc/`

`http://u6irlnorfxnn7cqs.onion/etc/`

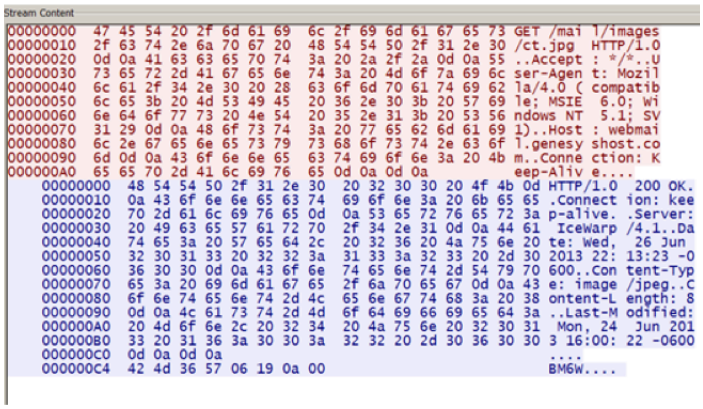
`http://snij5xfzt2qspxj2.onion/etc/`

Another interesting technical tidbit about these files is that all of the files except the final payload were packed using the infamous runtime packer Themida.

The final payload checks for a File Mapping Object, just like the March 20th wiper attack:

```
push    offset Name       ; "Global\\MicrosoftUpg
push    0                 ; bInheritHandle
push    4                 ; dwDesiredAccess
call    ds:OpenFileMappingA
```

After resolving the API address, it then created a thread to start communication:



The response data is split into two parts:

1. `BM6W`, which is the only command hard-coded in the binary:

```
push    4
lea     eax, [ebp+var_10]
push    offset aBm6w      ; "BM6W"
push    eax               ; char *
call    _strncmp
add     esp, 0Ch
push    esi               ; FILE *
test    eax, eax
jnz     short loc_1000117F
```

If the response data is anything other than `BM6W`, it will sleep, then try again.

2. `06 19 0a 00`:

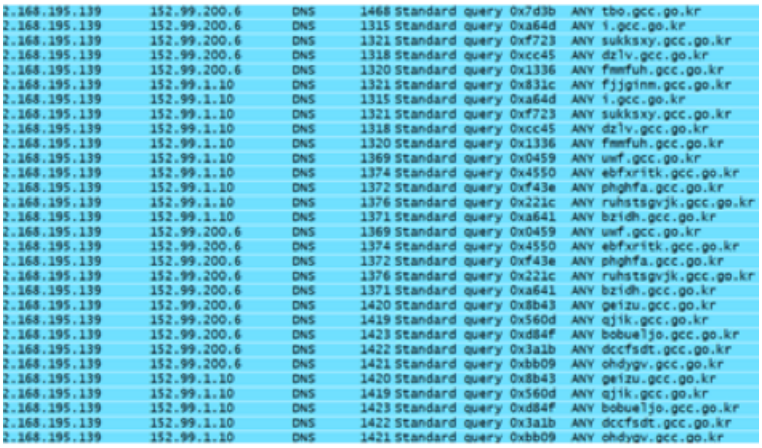
   - `0x06` – Month
   - `0x19` – Day
   - `0x0a` – Hour
   - `0x00` – Minute

Another time-bomb, just like the March 20th wiper attack!

If the system time has passed 10:00am June 25, it drops another file which was also packed by Themida:

```
push    offset aWuauieop_exe ; "\\
push    eax                  ; char *
call    _strcat
pop     ecx
pop     ecx
```

The attack payload then starts two threads to perform the DDoS attack by querying (random string).gcc.go.kr:



The two DDoS targets are hardcoded in the binary:

```
push    offset a152_99_1_10 ; "152.99.1.10"
mov     word ptr [esp+84Ch+var_83B+1], ax
```

```
push    offset a152_99_200_6 ; "152.99.200.6"
mov     word ptr [esp+84Ch+var_83B+1], ax
```

- 152.99.1.10 is the address of ns.gcc.go.kr
- 152.99.200.6 is the address of ns2.gcc.go.kr

You can read more on both of these attacks on the FortiGuard blog:

http://blog.fortinet.com/digital-attack-on-korean-networks-wipers-time-bombs-and-roman-soldiers/

http://blog.fortinet.com/6-25-DNS-DDOS-Attack-In-Korea/

About FortiGuard Labs

FortiGuard Labs compiled threat statistics and trends for this threat period based on data collected from FortiGate network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Services should be protected against the vulnerabilities outlined in this report as long as the appropriate configuration parameters are in place.

FortiGuard Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help protect against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, enabling Fortinet to deliver a combination of multi-layered security intelligence and zero-day protection from new and emerging threats. For customers with a subscription to FortiGuard, these updates are delivered to all FortiGate, FortiMail and FortiClient products.

Ongoing research can be found in the FortiGuard Center (http://www.fortiguard.com) or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog (http://blog.fortiguard.com).

About Fortinet (www.fortinet.com)

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise - from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, California, with offices around the world.

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480